Ref. Ares(2019)3748793 - 12/06/2019

RESIST

RESIlience enhancement and risk control platform for communication infraSTructure Operators

H2020-CIP-01-2016-2017
CRITICAL INFRASTRUCTURE PROTECTION
Grant Agreement No. 786409

RESISTO:

D10.10_EXPLOITATION ACTIVITIES-FIRST

RESISTO – This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No786409

RESISTO
D10.10 – EXPLOITATION ACTIVITIES – FIRST

Document Manager:	Federico FROSALI	LDO	Editor

Project Title:	RESIlience enhancement and risk control platform for communication infraSTructure Operators
Project Acronym:	RESISTO
Contract Number:	786409
Project Coordinator:	LEONARDO
WP Leader:	LDO

Document ID N°:	RESISTO_D10.10_190604_01	**Version:**	1.0
Deliverable:	D10.10	**Date:**	04/06/2019
		Status:	APPROVED

Document classification	**PUblic**

Approval Status	
Prepared by:	Federico FROSALI (LDO)
Approved by: (WP Leader)	Federico FROSALI (LDO)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	NA
Security Approval (Security Advisory Board Leader)	NA

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
All the partners	RESISTO CONSORTIUM	NA

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
PMT	RESISTO CONSORTIUM	NA
Markus MULLER	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.9	24/05/2019	All	All	Final draft
1.0	04/06/2019	All	All	Final release

COPYRIGHT STATEMENT

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, under the Grant Agreement No 786409.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

PROJECT CONTACT

LEONARDO
Via Puccini 2 – Genova (GE) – 16154 – Italy
Tel.: +39 348 6505565
E-Mail: bruno.saccomanno@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also extreme weather events and natural disasters represents a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. Through RESISTO Communications Operators, will be able to implement a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation.

EXECUTIVE SUMMARY

Market strategy, exploitation and sustainability, IPRs: initial plan, annual plan updates and reports, innovation management report and business plan refinements

CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone systems
API	Application Programming Interface
APN	Access Point Name
ASIC	Application Specific Integrated Circuit
B2B	Back-to-Back gateway
CCA	Critical Communication Application
CCS	Critical Communications System
DMO	Direct Mode Operations
ETSI	European Telecommunications Standard Institute
EU	European Union
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile communications
GSSI	Group Short Subscriber Identity
HW	HardWare
ISI	Inter System Interface
ISSI	Individual Short Subscriber Identity
ISITEP	Inter System Interfaces for TETRA-TETRAPOL Networks
ITSI	Individual TETRA subscriber Identity
LTE	Long Term Evolution (= 4G)
MNO	Mobile Network Operator
PC	Personal Computer
PPDR	Public Protection and Disaster Relief
PTT	Push To Talk
QoS	Quality of Service
SW	SoftWare
TCCE	TETRA and Critical Communications Evolution
TEA2	TETRA Encryption Algorithm #2
TETRA	TErrestrial Trunked RAdio

TG	Talk Group
TMO	Trunked Mode Operations
UE	User Equipment
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION

This deliverable addresses two main topics

- **the exploitation strategy and plan** of project results and future business opportunities in order to maximize the benefits that the partners may gain from the RESISTO outcomes. To this aim identification of high potential project results and specific form of exploitation both at consortium and individual partner level have is presented. A set of identified KPIs which will be used to continuously monitor the impact of the exploitation activities.
- **the innovation strategy and process** in order to keep up with technology innovation and market demand evolution focused in this phase on innovation management plan definition and preliminary benchmarking of the surrounding market solutions that RESISTO will have to confront.

2. EXPLOITATION

In this document, the plan for exploitation of the knowledge produced by RESISTO is presented, largely based on information available from the partners at the time of the submission re-elaborated in light of updates available at the beginning of the project. Specifically a study has been made to identify what the key ingredients are for RESISTO efficient exploitation. The document initially introduces general considerations addressed to broadly explain the foundations for the elaboration of the exploitation plan. Then, specific attention has been put on the applications envisaged by RESISTO.

2.1. Exploitation Plan

Exploitation is seen as a key enabler for the success of RESISTO. It is a paramount principal in exploitation activities to make use of the results of the project to create value within the participating organizations and thus to improve their competitive advantages.

The exploitation plan implements an incremental approach that will be developed alongside the lifespan of the project to follow up after the project's end

Figure 1 summarizes the overall logic and approach regarding the RESISTO exploitation plan and is a review and partial re-modulation of the plan already presented during the proposal stage.

Figure 1 – RESISTO Exploitation Plan

Phase 1 (D10.10, D10.11) is focused on:

- **Market analysis:** The potential market is reviewed and updated in the light of the evolution of the context and of latest available market data, and the refinement of RESISITO framework after the first design stages. The market defines, characterizes and segments the potential opportunities for different solutions developed in the project, as well as describe the value chains serving each technology.
- **Draft Business model(s):** preliminary business models introduced in the proposal stage are reviewed and consolidated taking into account the outcomes of the market analysis, the identified value chains and the intended customers for each developed product. The business models map how RESISTO can create and deliver value by identifying: (a) the relevant customers segments; (b) the value proposition; (c) the channels to deliver the value proposition to customers; (d) the resources required, (e) the activities to be performed and (f) the required partnership. The elements above will be used in phase 2 and linked to revenue and costs streams to quantify the business plan.
- **Preliminary Exploitation Plan:** Furthermore it will investigate possible elements for the success of the business model, such as the importance of relationships with customers, partners, providers and other key stakeholders, marketing activities and rasing awareness towards the project and its results
- **Preliminary Innovation management and IP Management Plan** : in order to keep up with technology innovation and market demand evolution focused in this phase on innovation management plan definition and preliminary benchmarking of the surrounding market solutions that RESISTO will have to confront.

Phase 2 (D10.12) will focus on the definition of:

- **Business Plan:** A business plan shall be defined including identified costs, the market analysis and the refined business models. Special attention shall be paid to value proposition, business models, target markets, timescales, competitors and risks assessment and estimated costs to assess quantitatively the financial feasibility of RESISTO quantifying initial CAPEX and OPEX vs. generated revenues through the time, based on realistic estimations of price and penetration. Different scenarios will be developed (optimistic, realistic and pessimistic).
- **Exploitation Plan Update:** review and update of activities to ensure the success of the business model (relationships with target customers, partnerships with technology providers and other key stakeholders), marketing activities review; identification of standardization needs that can contribute further to the development of the CIP initiative (special attention will been paid to standardization of the solutions proposed in the project with specific reference to the resilience analysis model)
- **Innovation management and IP Management Plan update:** update of the technological competitive landscape and identification of the most promising areas in terms of intellectual property rights protection aligned with project midterm results;

Phase 3 (D10.13),will focus on:

- **Business Plan refinement:** The business plan will be refined
- **Definition of a Marketing Plan:** The marketing strategy will be elaborated in the marketing plan e.g.; in terms of price, promotion, distribution approaches etc. Taking into account final

analysis and synthesis of project´ outcomes, the correct positioning for the products will be defined in this phase, based on their capability to satisfy user needs vis-à-vis the offer of competitors. Based on this assessment, coherent positioning choices (branding, product description) will be performed, to be taken into account in all Communication Activities.

- **Exploitation plan refinement:** final refinement of activities to ensure the success of the business model after the end of the project and to ensure a full market exploitation of RESITO platform and components. Side markets will be explored to identify further opportunities
- **IP Protection roadmap:** Activities and methodology defined in the IP Management Plan will be carried out at this stage when final products and outcomes of the project have been generated

A preliminary analysis of the market sector, the business model and value proposition will be dealt with hereinafter.

2.2. RESISTO Business Model and Value Proposition

Candidate RESISTO Business Models are here introduced to guarantee the medium and long-term economic sustainability of the product/service offering.
RESISTO is an innovative solution for Communication Infrastructure providing holistic (cyber/physical) situation awareness and enhanced resilience. RESISTO is intended to support Communications Infrastructures Operators to take the best countermeasures and reactive actions exploiting the combined use of risk and resilience preparatory analyses, detection and reaction technologies, applications and processes in the physical and cyber domains. Based on this proposition **RESISTO business model** must address different kind of customer segments: B2B (Business to Business): mainly Telco/Communication Operators but also other CI operators (managed security services); B2G (Business to Government) since protection of CI sites involves also National Governments and local institutions; S2B (Science to Business) to take into account technology innovation transfer from research institutions to industries as the case for the universities and research centres in the consortium (RM3, EMI, ICCS).
The most appropriate business models for the RESISTO platform identified at this stage are:

- **The system integrator business model**: Under this kind of model Large Enterprises like LDO and TEI, can provide RESISTO platform as a scalable solution/system customized on the end-user. This kind of model requires heavy investment in innovation, effective partnership with innovative technology providers and RTOs/universities, reputation in the field of CI protection and customer intimacy. The profit of this kind of model is high for high end (complex) solutions over large systems. This model represents a clear opportunity for technology providers (like GT, INT, TEI) and capability providers (RM3, ICCS, ADI, BSS) under the condition ob being able to keep up with the competition

- **The security as a service business model**. Telco operators already provide managed security services to their customers. RESISTO platform may be adopted by Telco operators (like TIM, BT, OTE ORO, RTV) to extend or reinforce their offering targeting their CI customers and largely leveraging on their customer intimacy. Large Enterprises with expertise in managed services like TEI, and CI protection may embrace this business model as well.

- **The service oriented business model**. This kind of business model includes consultancy service, design service, supervision service, training service, maintenance service. It is expected that consultancy, design and training services will be sold as part of the solution (to this regard the Cisia Pro tool and the modelling approach from EMI can be very powerful)

while supervision and maintenance services can be sold long after the delivery of the system. The profit of this kind of business model is higher in % compared to the previous model due to reduced investment required (mainly opex cost). The partner in the best position to exploit this business model are the Large Enterprises with expertise in the field of CI protection security management, like LDO; and managed security services providers like the telco operators (TIM, BT, OTE ORO, RTV) and TEI.

Go-to-market strategy - Major drivers for selling the RESISTO platform to the market are

- the ability to improve detection reaction and mitigation capabilities of the communication operators in the short term
- In face of complex cyber-physical attacks the ability to improve decision making process, leading to a more efficient selection and use of countermeasure and mitigation
- The ability to increase infrastructure resilience in the medium/long term

The main obstacle to RESISTO adoption relies in the need to integrate data from many different domains (cyber and physical), typically managed by different department in the same organization, implying the need to review also company processes and responsibilities.
As soon as the RESISTO platform integration steps will be completed and the IPR aspects agreed, the RESISTO platform can be proposed to a number of telco operators and CI operators in EU also leveraging on AB members involvement. Our first estimation is that in the EU exist more than **300 relevant authorities and participants** in this field. Another important dimension is that RESISTO will be available, as said, as either a stand-alone configurable platform, to be embedded on an end user infrastructure, or as a service.

Value proposition - The RESISTO value proposition covers the following areas

Internal benefits	External benefits
• Cost savings, protecting Telco infrastructures from potential damages and service outages coming from either combined and independent cyber and physical threats; • Enhanced Resilience, reducing the risk of service interruption toward their customers during terrorist attack and/or stress over the infrastructure due to natural disasters • Increasing incentives for cyber security, adopting standard certification and being compliant with European regulation;	• Maintaining competitive advantage for Telco operators; • Return on investment, selling security as service; • Increasing customer loyalty, selling not just the infrastructure but the security on that; • Extend Service offering building new relationship with suppliers and wider CI protection community

2.3. Preliminary Market Analysis

In order to estimate the business opportunity for RESISTO a preliminary market analysis is presented that takes in to account the overall value of global CI protection market and split it according to the different envisaged business models.

According to a LDO's market outlook, the consolidated global CI Security market is expected to grow from 77,32 B€ in 2016 to 106,3 B€ in 2022.The following table details the 2016-2022 forecast for the global CI security market split by product and system integration sales, service & upgrades, and planning, consulting & training.

Global CI Security Market	2016 (act)	2017 (act)	2018 (act)	2019	2020	2021	2022
Product and system integration Sales	39,4	41,9	44,7	47,5	50,7	53,7	56,6
Services & upgrades	34,0	27,5	30,2	33,3	36,6	40,0	43,6
Planning, consulting training	3,9	4,2	4,6	4,9	5,3	5,6	6,1
Total	**77,32**	**73,6**	**79,5**	**85,7**	**92,53**	**99,3**	**106,3**

Figure 2 - Global Critical Infrastructure Security Market Size [€B]

The global CI security market is predicted to grow steadily during the forecast period. The CI security service & upgrades revenues are expected to achieve the highest grow. They, as well as the planning, consulting and training market, will grow faster than the product sales.

Global CI Security Market	2016 (act)	2017 (act)	2018 (act)	2019	2020	2021	2022
Product and system integration Sales	6.5%	6.3%	6.4%	6.5%	6.6%	6.0%	5.5%
Services & upgrades	10.1%	9.8%	9.9%	10.0%	10.0%	9.4%	8.8%
Planning, consulting training	7.7%	7.8%	7.9%	7.7%	8.1%	7.5%	6.8%
Total	**7.9%**	**7.7%**	**7.8%**	**7.9%**	**8.0%**	**7.4%**	**6.9%**

Figure 3 - Global Critical Infrastructure Security Market CAGR

Product and system integration solution sales keep the lion's share of the global Critical Infrastructure Security market. The market shares of the market elements (i.e., product sales, service & upgrades and planning, consulting & training) are expected to change slightly during the forecast period. The market share of product sales will decrease gradually; as a result of a growing installed base the service & upgrades revenues share will increase. The market share of planning, consulting and training is expected to remain flat over the years.

Global CI Security Market	2016 (act)	2017 (act)	2018 (act)	2019	2020	2021	2022
Product and system integration Sales	57.7%	56.9%	56.2%	55.5%	54.8%	54.0%	53.3%
Services & upgrades	36.6%	37.4%	38.1%	38.8%	39.5%	40.3%	41.0%
Planning, consulting training	5.7%	5.7%	5.7%	5.7%	5.7%	5.7%	5.7%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Figure 4 - Global Critical Infrastructure Security Market Share [%]

Further refinement of these data, with specific reference to the TLC infrastructure protection, will be presented as part of the following deliverables (D10.11) leveraging of feedbacks from telco operators involved in the consortium and update market research datra.

2.4. Overall Consortium and Individual Exploitation Plan

Hereafter we describe how the project beneficiaries will benefit from and exploit the solutions developed in RESISTO. We expect that exploitation will be performed twofold: within the partners through the possibility to develop a joint proposition to the market, ideally at consortium level, promoting the RESISTO platform as a whole (or self-consistent parts of it), and at individual partner level, exploiting RESISITO as a way to market specific components, networking with partners and potential customers.

While we see a great potential for exploitation at consortium (or part of) level, as there is complementarity between competences and roles of the involved partners, especially among LEs, SMEs and RTOs that could implement an integrated offer (consulting plus turn-key solution), this requires the establishment of commercial agreements among the partners that we expect to be defined only at a later stage when the RESISTO framework has been validated and its value clearly expressed. In the meantime as part of the exploitation plan a strategy for possible consortium exploitation will be implemented working on:

1) Definition of models for a combined offer

2) Definition of a draft template for commercial agreement on exploitation of RESSITO framework and components

These two points will be developed as part of D10.12 and D10.13.

At individual partner level at this stage it's possible to present an overview of preliminary individual exploitation interests and strategies of each partner. Individual exploitation plan are split in two groups: LEs/SMEs/RTOs whose main target is to leverage on RESISTO to develop technology, skills and capabilities, establish relations with potential commercial partners and customers, build reference in the field of CI protection, and Telco operators that to the above mentioned target add the opportunity to test RESISTO solutions in their existing and future platforms promoting their image of innovative and "resilient" companies. The implementation of the individual plans in combination with the definition of an overall exploitation vision, will maximize the effectiveness of the project exploitation activities.

P.	Individual Exploitation Plan (short description) for LEs/SMEs/RTOs
1. LDO	LDO exploitation plan aims at increasing its expertise in the field of Critical Infrastructure protection, at innovating its systems and at increasing its position on the national and international CI market establishing links with a number of potential customers. LDO business model looks at the exploitation of the RESISTO platform results to enhance its product portfolio (with specific reference to SC2 solution and Security Governance Portal for cyber security) and introduce innovation solutions in current systems.
2. RM3	Over the last years, RM3 research group has been appointed as consultant for CIP and CIIP activities by several industrial and governmental entities thus acquiring a valuable knowledge about mechanisms and architectures of actual CIs both at national and European level. RM3 will exploit RESISTO results and contacts with end-users to further develop its consultancy services in the field of CIP and risk management. Athis stage RM3 also envisions the possibility to develope an industrial product based on CisiaPRo, through the collaboration with Leonardo adn other LES in the project
9. TEI	TEI is involved in developing Mobile Telecommunication infrastructure with a strong commitment on 5G evolution. RESISTO results in the field of security of telecom systems and of SDN and NFV in particular will be exploited in the development and extension of future TEI telecom infrastructure

	product portfolio. The Emergency Warning Communication Function validated in RESISTO will be exploited within the mission critical communication market. The collaboration with Leonard is seen as a great opportunity to this aim.
11. EMI	EMI cooperates with leading industrial companies. The planning supporting a nd disaster management tools developed and adapted by EMI to the Communication CI domain will be exploited both to reinforce and extend cooperation with industrial companies in the field of CIP and to enhance its IP (Intellectual Property) knowledge portfolio.
12. ICCS	RESISTO will give ICCS the opportunity to improve its position in scientific fields of anomaly detection, radio networks, 5G, sensors and signal processing. ICCS will exploit project results by pursuing patents applications, creating new research links, establishing further research collaborations within national and European projects, participating in exhibitions and related events, exploiting its connections with the Hellenic Public/Private Security Sector and Regulatory Bodies. It will give the opportunity to employ skilled researchers and PhD students contributing to further high-tech jobs creation on cutting-edge research topics.
13. BUW	BUW plans to complete the Ph.D. thesis (Sylvia Bach) during the project. Project results will be included in the safety engineering curricula of the university, especially in the courses „Organization and Communication in Crisis Management “and „Principles of Crisis Management“. It is assumed that the participation will strengthen the competencies of the institute in EU and international crisis management R&D.
14. CER	CER will evaluate potential adoption of RESISTO methodologies and approaches in order to promote them for certification and validation purposes inside its institutional activities.
15. INT	Through RESISTO, INT will have the opportunity to reinforce its leading position in the satellite spectrum monitoring market, offering commercial 5G network operations tools, also addressing new business models from being provider of complete packages towards offering of pluggable RF simulation and measurement components. The prototype of industrial IoT sensors validated in RESISTO will open to the company the appealing possibility of offering security solution for telecommunication physical sites protection improving also its professional consultancy services on the deployment of network system/applications.
16. GT	GT is the largest industrial blockchain platform provider, offering Keyless Signature Infrastructure (KSI) technology that enables massive scale data authentication without reliance on centralized trust authorities. GT is KSI technology provider to TEI and other telecommunication providers and partner in industrial blockchain commercialization. Through integrating KSI into the innovative RESISTO solutions, GT expects to get in touch with a number of new potential customers in the Telco sector and to promote its solution in the CI cyber protection market exploiting new commercialization opportunities.
17. ADI	ADI will exploit RESISITO results with reference to its solutions for video analysis and UAV detection with key stakeholders in Cypriot market and other areas where ADI operates (e.g. Balkans and Middle East): Cyprus Telecommunication Providers, in particular with Cyprus Telecommunications Authority (CYTA) with which ADI has a successful collaboration track; Office of Electronic Communications & Postal Regulations (OCECPR), ENISA national contact point of ENISA. ADI will promote RESISTO to the Cyprus Research Promotion Foundation, coordinator of the EEN Cyprus that is expected to offer collaboration and commercialization possibilities and potential joint ventures
19. BSS	BSS goal is to promote RESISTO platform to business customers that are operating Critical Infrastructures. BSS plans to use and engage its offensive, defensive and intelligence capabilities combining them with operations and innovative functionalities brought by integrating RESISTO ecosystem within its customers’ CIs systems. In this way BSS will develop new services for customers until this point not accessible.

Table 1- Individual Exploitation Plan for RESISTO LEs/SMEs/RTOs

P.	Individual Exploitations and/or Potential Adoption Plan (short description) for End Users
3. TIM	TIM, being an international infrastructure operator and TLC-ICT services provider, has interest in exploiting RESISTO results internally and in the market. RESISTO solutions will be included in its existing and future platforms, with the aim of enhancing their security with clear positive impact on its image. RESISTO adoption will also help TIM to comply with the Directive 2009/140 EC. TIM also will exploit RESISTO in the service offering in the 5G area (e.g. 5G for Italy), and extend its Managed security services portfolio
4. OTE	Based upon technical and market-led priorities, OTE aims to exploit RESISTO results into its existing and future network/service solutions, thus strengthening customers' confidence and enhancing its competence in the field of telecommunication networks security. OTE intends to promote a policy that will be beneficial for the company, also within the broader Deutsche Telekom Group. The RESISTO's results will also help to design and promote new business models
5. BTC	BTC expects to incorporate the project results in evolved and extended versions of its unified Cyber Security Platform (CSP). CSP is used to implement its own cyber self-protection and as a basis for managed Cyber Security Operations Centre services for major public and private sector customers.
6. ORO	ORO will promote RESISTO platform as a service towards the business customers operating CIs such as utility (water, gas, energy) providers in line with ORO cyber security strategy and ORO cyber security solutions portfolio including the Security Operation Center (SOC) and security solutions for Industrial Control and Metering Systems. RESISTO innovative functionalities will be integrated in ORO SOC. ORO will also promote RESISTO at France Telecom group level
7. RTV	RTV will exploit RESISTO to set up a platform to protect its internal infrastructures and RTV's Maritime critical infrastructure to enhance its resilience. Moreover in full synergy with 5G City project RTV will exploit RESISTO results to secure the LTE-PPDR virtual slicing system to provide to the Mission Critical market the most secure and performant broadband connectivity service.
8. ALB	ALB will exploit RESISTO results by leveraging their products and services in the 5G area, to enhance security and reliability of its offering.

Table 2- Individual Exploitation Plan and/or Potential Adoption Plan for End Users

3. INNOVATION MANAGEMENT

The Innovation Management is a complex process related to those management activities that, starting from end users' needs, aim to continuously identify and check new ideas with the final objective of developing new products or services which can satisfy those needs. In a sense, Innovation Management cyclically starts when the creative activities start, and finishes when a concrete result (either a product or a service) is deployed.

Traditional activities of the Innovation Management process are:

- Identify and continually manage an overall innovation approach
- Understanding market needs and opportunities
- Continually monitoring the landscape (market and technologies)
- Assess the innovation potential of research results
- Drive the project development plans to better meet the market expectations

These activities are cyclically executed, to be in line with the evolution of the market and technological landscape. Once defined an overall innovation strategic approach which drives the activities and defines the roles of involved actors, the activities start monitoring the market needs and opportunities, comparing them with already available technological solutions, to identify new opportunities for innovative products/services which can fill the gaps.

This is done with a continuous interaction with the research and development teams, trying to adapt the development plans with an evolving context of market expectations and constraints, technologies, competitors, IP protection mechanisms, social/ethical aspects, regulations and standards.

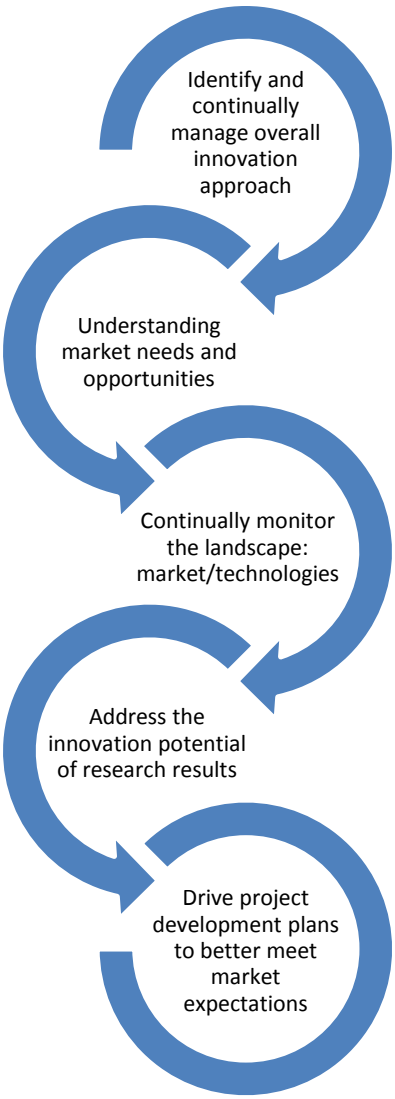

Figure 5 - Innovation Management Process

3.1. Elements of innovation in RESISTO Project

In the following paragraphs, we report the current key potential innovation elements characterising the RESISTO platform, comparing them with the technological State of the Art [SoTA] and putting in evidence their more distinguishing features. These key innovation elements and their features are reported as envisaged at the beginning of the RESISTO project, and probably they will be adapted/added/deleted during the project progress to follow changes in the demand/market and/or in the technological landscape (new disruptive technologies). For this, the market and technological landscape will be continuously monitored as a critical innovation activity to better react to possible changes to the market needs, to the contextual constraints or to the available technological solutions.

Aware that the protection of Communication CIs is a crucial topic for the European society, the main ambition of the RESISTO consortium is to develop the necessary concepts and a solid technological baseline to create a comprehensive solution that allows faster detection of new cyber/physical threats, better informed decision making and achievement of a joint understanding of cascading effects within the CI an across interconnected CIs providing enhanced resilience of Communication Infrastructure and CIs that rely on it.

The technological components that are part of RESISITO platform encompasses novel horizontal functionalities on one side (i.e private blockchain, Software defined security, UAV detection) and the innovative integration/use of technological modules on the other (i.e holistic system modelling, cyber-physical correlation, ….). This unique combination will enhance the effectiveness of the RESISTO solution for the Communication CI's protection while simultaneously advancing the related State of the Art (both per individual module and in a holistic level).

3.1.1. Cyber-physical Risk/Resilience assessment of Communication infrastructure

The role of the Data Integration Layer is to act as the middleware component of the RESISTO platform. It is meant to receive and dispatch all information among RESISTO components and between the RESISTO platform and all external systems.

It provides infrastructural and communications services to functional components and for this reason a detailed description is provided in chapter 5, dedicated to explaining the communication methods that have been chosen both for the interaction between the internal components of RESISTO and for communications with external sources.

3.1.2. Holistic System Modelling and interdependency simulation analysis for Risk Predictor

State Of The Art. The approach proposed by RESISTO in the field of *performance degradation modelling and simulation* covers the time-dependent analysis of interdependencies of different system layers and level such as Physics, Cyber, Logic and Geographic, modelling infrastructure on an abstract level. The CISIApro simulator[1] (Critical Infrastructure Simulation by Interdependent Agents) analyses the effects of failure both in terms of faults propagation and with respect to performance degradation and effects of mitigation, in particular response and recovery. Currently such abstract models are not directly linked with models with higher resolution that allow to predictively assess the effect of natural and man-made physical but also cyber threats. Existing physical damage models or investigations for telecommunications subsystems cover, e.g., seismic[2], heavy storm[3], ice rain[4] but also (terroristic) explosive loading[5], impact[6] and flooding. Possible effects of drones are known[7], also

[1] http://cisiapro.dia.uniroma3.it/
[2] K. K. Sharma, S.K. Duggal, D. K. Singh, A.K. Sachan, Civil Engineering and Urban Planning: An International Journal (CiVEJ) vol.2, no.3 (2015), pp. 13-31.
[3] G. Ghodrati Amiri, Computers and Structures, vol. 80, no. 03, (2002), pp. 349-364, http://www.sciencedirect.com/science/article/pii/S0045794901001754
[4] N.D. Mulherin, Cold Regions Science and Technology, vol. 27, no. 2 (1998), pp. 91-104, http://www.sciencedirect.com/science/article/pii/S0165232X97000256
[5] Mark G. Stewart, Michael D. Netherton, David V. Rosowsky, Natural Hazards Review, vol. 7, no. 3 (2006), pp. 114-122, http://ascelibrary.org/doi/abs/10.1061/(ASCE)1527-6988(2006)7:3(114)
[6] C. U. Penalba, New Orleans Structures Congress (1999), https://trid.trb.org/view.aspx?id=511641
[7] See e.g.: http://www.business-standard.com/article/news-ians/interpol-warns-of-drone-attacks-by-terrorists-on-critical-infrastructures-117021400178_1.html

shelling occurred in similar cases[8] but are respectively much less investigated. By now tools with drag and drop capability exist that allow for the assessment regarding, e.g. explosive and seismic threats.

Progress Beyond State Of The Art. RESISTO uses models and engineering-simulations to refine and develop telecommunication subsystem damage and resilience behaviour models sufficient for predictive assessment regarding critical risks as put forward by the sample cases, in particular out of the set (terroristic) explosions, effects of drones, impact, cyber induced effects, and seismic. It starts out with existing structural model inventories adding typical nodes and edges of Telecommunication CI, e.g. sending masts, ground stations, backbone-components. Based on CISIA Pro modelling and integrated cyber-physical correlation the project can deliver an innovative solution for Telco CI protection governance that thanks to the flexible modelling can be easily extended to a wide range of Cis.

3.1.3. Cyber-Physical correlation

State Of The Art Most TLC enterprises have a SOC (Security Operation Centre) for the logical protection of the infrastructure and different systems (CCTV, Access control, Intrusion detection, biometrics etc.) for the physical security management and, in some cases, a PSIM (Physical Security Information Management) the integration platform for a single monitoring and control centre. So risk and threat scenarios as well as solutions for the protection of two domains are well known and implemented. In each domains the systems or platforms for the protection include specific modules for the correlation of information: cyber security uses this approach to improve significantly the detection of anomalies and attacks; one of main characteristics of PSIM systems is the correlation capability to integrate data from various systems in order to automatically identify situations and then gradually update those situations[9].

Progress Beyond State Of The Art The RESISTO platform adopts the approach of information correlation to data coming from two fields traditionally separated; besides the correlator will apply the deterministic pattern-matching algorithm to detect a specific threat situation and the not deterministic techniques (Artificial Neural Networks e.g.) to update incrementally the rules and thresholds on the basis of data collected from the ICT systems and the sensors/systems for its physical security. This allows for early detection of a new class of threats (i.e an employee entering a room with restricted access – physical- and then logging into a high security system with non-personal credentials – logical) combining physical and logical means so far largely underestimated and normally seen as disjoined.

3.1.4. Software Defined Security

State Of The Art*:* The SDN architecture with its separation of data and control plane from network devices drastically simplifies configuration and management of security policies, with significant reduction of security risks associated to policy inconsistency. On the other hand, the main SDN benefits pave the road to new attacks exploiting the vulnerabilities associate to softwarization and centralized control. Since OpenFlow is the most diffuse protocol for SDN implementation and deployment, research on SDN security mostly addressed OpenFlow based solutions. Recently, based on the softwarization trend that is pervading every element of a communication network, as witnessed by the reference documents published by 5G-PPP and NGMN Alliance, the Software Defined Security (SDS) paradigm has been introduced. Among the SDS solution we cite Catbird[10], OneControl[11] and OpenSec[12]. Solution proposed in literature have been focus on cybersecurity. The SDS paradigm is

[8] See e.g.: https://en.wikipedia.org/wiki/Metcalf_sniper_attack
9 Frost&Sullivan "Analysis of the Worldwide Physical Security Information Management Market" M683-11 November 2010
[10] "Private cloud security, a catbird white paper," Catbird Networks, Inc, white paper, 2014.
[11] "Netcitadels onecontrol platform the key to intelligent, adaptive network security," NetCitadel, Inc, white paper, 2012.
[12] A. Lara, B. Ramamurthy, "OpenSec: Policy-Based Security Using Software-Defined Networking", IEEE Trans.On Network And Service Management, Vol.13, No.1, March 2016

being successfully experimented by TRE and LDO in the H2020 Atena project (www.atena-h2020.eu).

***Progress Beyond State Of The Art**:* One major progress beyond the state of the art proposed by RESISITO is the extension of the SDS architecture in order to manage virtualization of both cyber and physical security. Concerning physical security virtualization it essentially applies to the logical controllers of physical security mechanisms involving programmable devices (e.g. video surveillance, electronic access control). The major difference between the ATENA and the RESISTO consists in the number of nodes and in the variety of security functions to be virtualized being ATENA simpler in terms of both nodes and functions. Thus the progress beyond the state of art will concern scalability of the solution, policy management, inclusion in the virtualized functions of those related to physical security as well as of those security functions related to wireless channels, with emphasis to functions pertaining to Physical and Logical Link layers, Radio Resource management and Mobility Management. In addition, the SDS architecture will be extended in order to fully support 5G communications, slicing and multi-tenant solutions included.

3.1.5. Blockchain for Data integrity

State Of The Art Traditional solution for data authentication which relies on centralized trust authorities (Public Key Infrastructures – PKI) suffer from problems of scalability and resilience (single point of failure). Furthermore, data integrity relies traditionally on the 'hardened box' concept where perimeter security keeps 'bad' actors out and 'good' actors in. Data transferability is facilitated by checksums and key-based digital signatures, which rely on trusted functions like key management, certification infrastructure and providing root of trustGuardtime's KSI blockchain technology enables massive scale data authentication without reliance on centralized trust authorities. KSI ensure data integrity, traceability, provenance and auditability along all the data lifecycle (processing, formatting, logs etc.). All the data changing history and logs integrity can be retrieved from the blockchain security solution and the data validity, time of change and signing entity is ensured in a way that third party validation independent from system can be used.

***Progress Beyond State Of The Art**:* RESISTO will integrate an innovative mature blockchain technology into its system which is provided by Guardtime. KSI is an industrial scale full stack blockchain infrastructure[13], the deployment of which offers a myriad of new security solutions[14] and service revenue opportunities for telecom operators. It will enable the telecommunications providers in the RESISTO platform to guarantee the state of their network without relying on trusted administrators or the procedures that define the security of their network.

3.1.6. Machine Learning for Threat Intelligence

State Of The Art. The threat landscape continues to grow and evolve in speed, sophistication, and persistence of attacks. Cyber threat actors are constantly developing new tactics, techniques, procedures, and the companies are forced to counter these new threats with new techniques and cutting-edge technology. Traditional security such as signature-based attack detection is still widely used. Its main limitation is the inability to detect attacks exploiting previously unseen patterns. To face zero-day threats and APTs (Advanced Persistent Threats) the scientific community has developed technics based on gathering and analysing raw data about existing or emerging threats and malicious actors from several sources (Threat Intelligence) as well as on the continuous monitoring of the

[13] Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees. Ahto Buldas, Andres Kroonmaa, Risto Laanoja. Hanne Riis Nielson, Dieter Gollmann. Secure IT Systems - 18th Nordic Conference, NordSec 2013, Proceedings. LNCS 8208, Springer, 2013.
[14] Efficient Record-Level Keyless Signatures for Audit Logs. Ahto Buldas, Ahto Truu, Risto Laanoja, Rainer Gerhards. Karin Bernsmed, Simone Fischer-Hübner. Secure IT Systems - 19th Nordic Conference, NordSec 2014, Proceedings. LNCS 8788, Springer, 2014

system behaviour in order to detect anomalies and malfunctions. The main drawback of this approach, when performed by ordinary means, is constituted by the very high false positive and false negative rates corresponding to an acceptable detection probability. There are some threat intelligence platforms that apply Machine learning technology such as Recorded Future[15] but since the attackers are evolving constantly it is necessary to keep improving this technology, allowing to process more information in less time and to reduce as much as possible the number of false positives. However, According to the report "Who's using Cyber threat intelligence and how?" by SANS[16], the majority of organizations are not yet mature at using Cyberthreat intelligence and only a small percentage of companies is using machine learning for supporting their threat intelligence processes.

Progress Beyond State Of The Art: The innovative approach is based on a combination of open source intelligence (OSINT) techniques crawling threat intelligence sources, combined with machine-learning algorithms for mining and filtering large amounts of data. Different types of threat intelligence sources, both public sources and private ones (commercial, provided by a customer or foreground source, e.g. incident response) will be crawled, and information gathered will then be filtered to detect threats that could potentially have an impact in the operator or their customers. The Machine learning algorithms will estimate a risk score for different entities such as IPs, domains, files or emails based on its history and relationship to other known malicious entities.

3.1.7. Airborne Threats (UAVs, drones) detection and tracking

State Of The Art: In light of the emerging use of unmanned devices, small UAVs or drones, are nowadays more and more considered as potential human-driven physical threats. Anomalies and airborne threats to specific telecom CIs (i.e., remote antenna parks and/or telecom pillars on high rooftops) are mainly monitored through visual methods (i.e. cameras); the threat has to be in rather close proximity to be detected which leaves less time for reaction. On the other hand, airborne anomaly detection tools based on active and passive sensors, exploiting mainly the electromagnetic (EM) spectrum i.e. radars, are mainly used in defence applications resulting in expensive dedicated equipment. Doppler radar is able to detect and track fast moving targets obtaining good visibility in harsh conditions (dusk, rain or snow); however, radar detection ability depends on the target's RCS (Radar Cross Section). Alternatively, acoustic sensors have many advantages that include non-line-of-sight, omni-directionality, passiveness, low-cost and low-power, playing a potential key role in situational awareness[17]. However, acoustic sensing depends on the environmental conditions and related sources of acoustic attenuation (e.g., temperature, wind speed and direction). Newest technology trends show that detecting low RCS moving targets can be made feasible by implementing mixed techniques[18]; these emerge as a promising detection solution while they can be combined afterwards with visual methods (i.e. cameras).

Progress Beyond State Of The Art: To this respect, in the framework of RESISTO, combination of active and passive sensors is proposed to overcome the inherent limitations; therefore they can be effectively used for detection of moving airborne targets, especially with low RCS providing additionally situational awareness and perimeter defence against low-flying threat aircrafts. To this end, detection with Doppler radar and acoustic sensors will be employed, based on existing ICCS' laboratory prototypes[19,20]. Potential intrusion events will be extracted from the combination of EM radar echo signals and acoustic data in order to finally detect, discriminate and report the presence

[15] https://www.recordedfuture.com/
[16] https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767
[17] T. Pham & L. Sim, "Acoustic detection and tracking of small, low-flying threat aircraft," 23rd Army Science Conf., Orlando, FL, 2002
[18] W. Shi, G. Arabadjis, B. Bishop, P. Hill, R. Plasse and J. Yoder, "Detecting, Tracking, and Identifying Airborne Threats with Netted Sensor Fence", The MITRE Corporation Bedford, Massachusetts, U.S.A, 2011, Chapter in Book: "Sensor Fusion - Foundation and Applications", Dr. Ciza Thomas (Ed.), ISBN: 978-953-307-446-7, InTech,
[19] Kyritsis Al., "Active and Passive Methods for Detecting small unmanned aerial objects", Diploma Thesis, Microwaves & Fiber Optics Lab, National Technical University of Athens, July 2016, Supervisors: Nikolaos K. Uzunoglu, R. Makri
[20] Al. Kyritsis, R. Makri, M. Gargalakos and N.K. Uzunoglu, "Active and Passive Methods for the Detection of Drones and Small Airborne Objects", 4th International Conference on "Operational Planning, Technological Innovations and Mathematical Applications OPTIMA 2017" 25-26 May 2017

and movement of potential moving airborne threats, UAVs and drones, for target detection, reducing false alarms ratio and improving the anomaly detection accuracy and reliability. Radar and acoustic signal processing techniques will be assessed and implemented including: beamforming, frequency domain thresholding, Hough transform based techniques for acoustic signature detection, Support Vector Machines (SVM) and Naive Bayes Classifiers (NBC) for target classification as well as Kalman filtering for tracking. Various algorithms are used in order to reach optimal combinations: probabilistic data association for measurements under high clutter presence, interacting multiple models algorithms on targets' higher order movements, extracting the target's track from range and Doppler shift measurements.

3.1.8. Innovative secure IoT for physical security

***State Of The Art**:* Industrial IoT nodes today present varying and sparse security functions not fully integrated with datalinks and are not widely used in telecom infrastructure protection[21]. Some IoT-specific networks such as those of LPWAN class enjoy inherent security characteristics (e.g. transmit-receive decoupling in SIGFOX), but a complete security solution still does not exist due to interoperability, cost or complexity-avoidance reasons. Several recent attacks have raised concerns about the overall security of IoT and its adequacy for industrial contexts[22].
No permanent smart spectrum surveillance capability is commonly deployed at telecom radio sites today. Only specialised radio surveillance missions are activated when significant interference is (indirectly) detected though network equipment monitoring. Specialised companies contracted ad-hoc perform radio surveys using normally expensive portable instruments, which is both expensive and useless in case of purposely planned, elusive radio threats which can be executed with extremely low cost hardware and limited knowledge thanks to today SDR equipment and related software frameworks[23].

***Progress Beyond State Of The Art**:* INT will develop a class of Industrial IoT nodes for physical access security with security-by-design principles based on the SECWAT sensor prototype developed by INT in the frame of the Spanish National 3S-CS project. The IoT node features full lifecycle handing of security functions: firmware/keys provisioning, protection of data (at-rest and in-transfer), firmware integrity and updates check; authenticating in every step the peer interacting nodes. The key technological components of the sensor is a crypto-chip providing a secure execution and storage environment and a dual-link capability (LPWAN + BLE) able to operate in harsh environments and including a secure execution environment for crypto-key and software integrity protection. In RESISTO the IoT node will be developed in two versions: one featuring a smart lock for physical access control and another one featuring tamper detection of network equipment. Moreover within RESISITO a Smart Spectrum Surveillance module (S3 module) will be developed and integrated to be collocated with telecom radio sites, taking benefit of operator information related to the "normal conditions" of the radio spectrum around the monitored station. The S3 module will include automated functions to: (i) detect rogue user-facing and backhaul facing 4G radio nodes; (ii) detect smart jamming to the user-facing 4G radio interface; (iii) detect suspicions radio activity around the monitored site which may point to wireless data exfiltration devices installed by intruders or different threat to auxiliary networks used at the site (e.g. SIGFOX, BLE); (iv) perform generic multi-band radio activity profiling to assist in the detection of yet unknown threats. This set of capabilities represent a clear advance compared to the existing means used by telecom operators to detect radio-related threats around their sites.

[21] Strategic Principles for Securing the IOT; U.S. Department of Homeland Security
[22] Protecting operational technology from cyber-attacks https://www.cgi.com/sites/default/files/white-papers/convergence-security.pdf. last accessed 08/ 2017
[23] Shaik, A.; Seifert, J.; Borgaonkar, R.; Asokan, N.; Niemi, V. Practical Attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems. In Proceedings of the 23nd Annual Network and DistributedSystem Security Symposium (NDSS 2016), San Diego, CA, USA, 21–24 February 2016

3.1.9. Audio and visual analytics

State Of The Art: Video and Audio sensors are widely used in surveillance operations and protection of critical infrastructures. Intelligence algorithms are applied in audio and video streams for the real-time detection of events for the early identification of illicit activity. Pattern recognition and machine learning techniques are used to extract acoustic events (i.e. gunshot, screaming, glass breaking) or to classify persons, vehicles and other objects that are moved within the controlled by the infrastructure area. Upon an event detection by analytics algorithms, a video clip is generated and delivered to the security operator. Security operator is notified with an alert about the suspicious activity and with important information about the event (location, etc.). This intelligent process reduces the effort of the operator by monitoring in a 24/7 base a huge number of sensors. Additionally, the early detection of events (real-time) and the ability to extract semantic information (i.e type of event, illegal access in restricted area, location of the event) can provide useful data to event processing and correlation platforms for further analysis.

Progress Beyond State Of The Art: In RESISTO, beyond the acoustic event detection, audio analytics are enhanced with techniques capable for localization of the source of the detected event. This feature can be used as an input to the video sources (CCTV) cameras in order to adjust the position to the source of the acoustic event. The added value of this integration (between audio and visual sensors) in the ability to provide to the security operator a real-time picture of the field where the event occurred. Furthermore, cross-correlations of audio and video analysis results will be developed in order to provide more accurate and precise alerts.

3.1.10. Emergency communications – Emergency Warning Communication Function

State Of The Art Alert sharing information systems and emergency apps are already available, but often they aren't used in the proper way and they aren't integrated with systems to detect automatically physical and cyber-attacks. Available emergency apps are designed to be "over the top" and often they aren't scalable. A lot of emergency systems was developed after 9/11 terroristic attacks. Often these systems have proven to be unreliable as in the case of France's government's instant message app during recent Nice attack[24] or American Federal Communications Commission initiative "FirstNet" envisioned as a way for police and firefighters to communicate implemented with obsolete technologies and it's not up and running after four years of development[25]. Communication with populations and specific teams in the event of an attach to a critical infrastructure could be made using local messaging based on the network proximity[26], but solutions that have been implemented do not integrate locations information available on the devices (eg. GPS) with that available at telecommunications nework layer.

Progress Beyond State Of The Art RESISTO develops an innovative "Emergency Warning Communication Function" that will allow to define specific categories of users (such as rescue teams, security officers, neighbouring population, etc.) based on specific target areas (e.g group of mobile cells, geographical perimeter, etc.), and send them relevant information when events like natural disasters, physical or cyber-attacks occur. Alerts in specific areas using location information coming from the smart devices and/or telecommunication network will be implemented. The function can be integrated in 5G networks as well as in existing telecommunications networks and it can be made available "as a Service" to specific public safety agencies. High availability, scalability and interoperability will specific feature of the technology.

[24] France's Saip emergency smartphone app failed during Nice attack
[25] The $47 Billion Network That's Already Obsolete - https://www.theatlantic.com/magazine/archive/2016/09/the-47-billion-network-thats-already-obsolete/492764/
[26] Namiot, Dmitry, and Manfred Sneps-Sneppe. "Local messages for smartphones." Future Internet Communications (CFIC), 2013 Conference on. IEEE, 2013

4. REFERENCES

INDEX	REFERENCE
[Ref1]	RESISTO – Grant Agreement. Project Starting Date: May, 1st 2018

Table 3- Reference Table